Content Authentication and Tamper Detection in Digital videos

A BACHELOR'S MINI PROJECT

INDIAN INSTITUTE OF INFORMATION TECHNOLOGY ALLAHABAD

B. Tech. - 7th Semester (IT)

Under the Guidance of:

Dr. Vrijendra Singh

Submitted by :

Rahul Gupta	**(RIT2011050)**
Amit Kumar	**(RIT2011051)**
Prashant Joshi	**(RIT2011056)**
Prakhar Solanki	**(RIT2011076)**
Akshay Gupta	**(RIT2011088)**

ACKNOWLEDGEMENTS

We would like to express our sincere gratitude to Dr. Vrijendra Singh for providing the opportunity to work under his guidance for 7th semester project.

We also like to thank him for his support and guidance throughout the process of project making.

Place: Allahabad
Date: 4 December, 2014

Rahul Gupta
Amit Kumar
Prashant Joshi
Prakhar Solanki
Akshay Gupta

CERTIFICATE

This is to certify that this project report entitled “Content Authentication and Tamper Detection in Digital Videos” submitted to Indian Institute of Information Technology, Allahabad is a bonafide report of work done by Rahul Gupta, Amit Kumar, Prashant Joshi, Prakhar Solanki and Akshay Gupta under my supervision from July 2014 to December 2014.

Place : Allahabad	Signature of supervisor
Date : 4 December, 2014	**Dr. Vrijendra Singh**

Table of Contents

1. Introduction

The amount of digital video that is available has increased the last few years, but the tools available for browsing video remain quite primitive.

Computer vision techniques promise to allow content based browsing of image sequences.

Motion based compression algorithms like MPEG can obtain higher compression rates without sacrificing quality. When the locations of scene breaks are known, knowledge about scene breaks can be used to look for higher level structures such as a sequence of cuts between cameras or to ensure that key frames come from different scenes.

This report presents algorithms for detecting and classifying scene breaks including (insertion) in digital video sequences.

We start with a survey of work on scene break Detection. These methods rely directly on intensity data and have difficulty with dissolves and with scenes involving motion.

We show that our methods have substantial tolerance for compression artefacts.

We present empirical evidence that our algorithm can outperform conventional approaches, especially on images involving motion.

1.1 **Currently existing technologies**

Computational schemes for detecting scene breaks generally define a similarity measure between consecutive images. When two consecutive images are sufficiently dissimilar, there may be a scene break. Typically similarity measure is threshold.

Several algorithms for detecting cuts and dissolves have been coined. These methods have relied directly on intensity data, and have used such technologies as image differencing and intensity histogramming, and concentrate on cuts.

Existing work has focused on cut detection which can be done with reasonably accuracy with a variety of simple schemes. There also has been work done on detecting dissolves, which itself is a herculean task in itself. All the algorithms till now rely directly on intensity.

A particularly interesting approach has been taken by Zhang, Kankanhalli and Smoliar. They have extended conventional histogram based approaches to handle dissolves and to deal with certain camera motions.

They use a dual threshold on the change in the intensity histogram to detect dissolves.

In addition they have a method for avoiding the false positives that result from certain classes of camera motion such as pans and zooms.

1.2 Motivation

There’s a need for authenticating a digital video by giving the following examples:

1.) A video clip can be doctored to defame a person. On the other hand, criminals get away from being punished because the video showing their crime can’t be proved trustworthy in the court of law.

2.) In surveillance systems, it is hard to reassure that the digital video produced as evidence is the one that is actually shot by the camera.

3.) A journalist cannot prove that the video played by a news channel is trustworthy.

4.) A video viewer who receives video through a communication channel cannot ensure that video being viewed is really the one that was transmitted.

So there is a compelling need for video, wherever it is and in whatever form it is, be made authenticable before use.

1.3 Applications

Our method can be used in the following three different kinds of scenarios:

1.) In the scenarios where video is streamed through a communication channel, due to the large size of video data, the streaming often suffers from congestion problem at the bottlenecks on the network. To overcome the network congestion problem, some data loss (e.g. loss of few video frames) is common. For instance, the video transcoder or the designated router intentionally drops frames to save bandwidth or to avoid buffer overflow.

2.) The proposed method is also useful in video identification. Video identification refers to a process that recognizes the existence of a particular video clip in large set of video data. For example, in an advertisement monitoring scenario where a commercial company or an individual can automatically identify in real time whether or not a TV channel is playing their video advertisement for the stipulated time. A TV channel may cut few frames to earn more time and the money. Our method can detect this type of tampering.

3.) Detection of object/region (such as human faces) tampering in a video is another application where our method can be used. The proposed method localizes the important spatial regions in a video and assigns higher weights to them in the authentication process.

2. Problem definition and scope

Now days there are lots of software's available in the market for editing videos.

We are, through this project, trying to identify whether there is a tempering done in the given video or not.

There are many ways in which a video can be tempered-

1. Cutting
2. Fading:
   2.1. Fade in
   2.2. Fade out
3. Inserting a Frame
   3.1. Insert a different frame into a video somewhere in between a video
   3.2. Dissolve a frame in video

- 1. **Cutting**:

When a frame or a sequence of frames is removed from video then this type of tempering is known as cutting.

This causes a sudden change in intensity and hence in pixel values, so it can easily be identified by looking at pixel change.

- 2.**Fading**:

When a frame is slightly inserted or removed so that user may not see the drastic change between the two frames then such type of tempering is known as fading.

There are two types of fading:

2.1. Fade In
2.2. Fade Out

2.1. Fade In:

When a frame is slightly inserted into the video, then this type of tempering is called fade in.

2.2. Fade Out:

When a frame is slightly removed from the video, then this type of tempering is known as fade out.

3. **Frame Insertion**:
There are two types of frame insertion:

3.1. When a new or different frame is inserted into a video at any place that comes under frame insertion tempering. In this case, like in cutting tempering, a sudden change in intensity in pixel values can be observed and hence can be detected easily

3.2. Dissolve:
When a frame is smoothly replaced by another one or sequence of frames is inserted in order to insert a frame so that there is not a big change in pixel values between two consecutive frames. This type of tempering is known as dissolved tempering.

Here we deal with only those tempered videos which are tempered by insertion.

Scope

- Now a day’s videos are being used as solid proofs in any judiciary system including USA. So it becomes very necessary to guarantee that the video is being used for such purposes to be authentic.

- Any malicious person can alter in such a video and can play with anyone’s life.

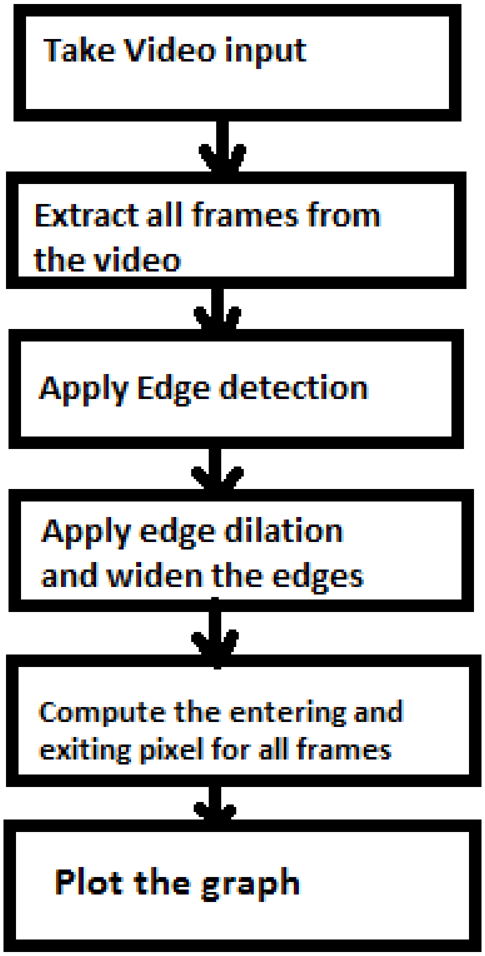
- In banking system also monitoring of activities in the banks are done through surveillance cameras so authentication of these videos are also necessary.

3. Literature Survey

SNo.	Name of the Paper	Date	Technique Used	Limitations
1	Scene Break Detection & Classification in Digital Video Sequences.	April, 1999	Tamper detection using exiting and entering edge pixels.	Unable to detect very minute tamperations.
2	Review of Robust Video Watermarking Algorithms	3 March, 2010	Watermarking based on MSB of watermark image.	Unable to do a real time watermarking
3	Exploring CDMA for watermarking of digital video	25 Jan, 1995	Combine multiple signals that overlap in both time and frequency yet remain separable.	varied and complex nature of attacks on watermark removal goes beyond the known problems that conventional CDMA signals have to cope with
4	A feature based algorithm for detecting and classifying scene breaks	April 1997	Incorporating algorithm into a browser for MPEG videos which allows the user to search for scene breaks	algorithm is not having higher search capabilities.

4. Proposed approach

4.1 Tamper Detection in Videos


Take Video input
Extract all frames from the video
Apply Edge detection
Apply edge dilation and widen the edges
Compute the entering and exiting pixel for all frames
Plot the graph

Flowchart of proposed method

- A video is taken as input, and all the frames are extracted.

- Edge detection is done for all the images using Sobel Edge detector. After the edge detection, the frame becomes as shown in figure

Original image

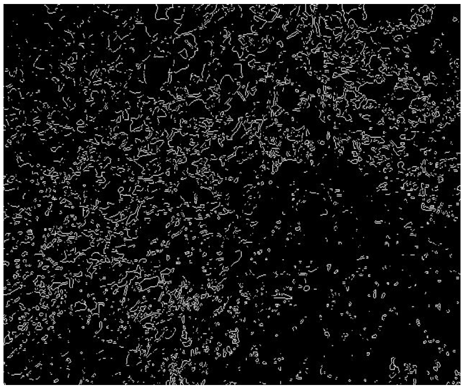


image after edge detection

- After edge detection, dilation is done to widen the edges.

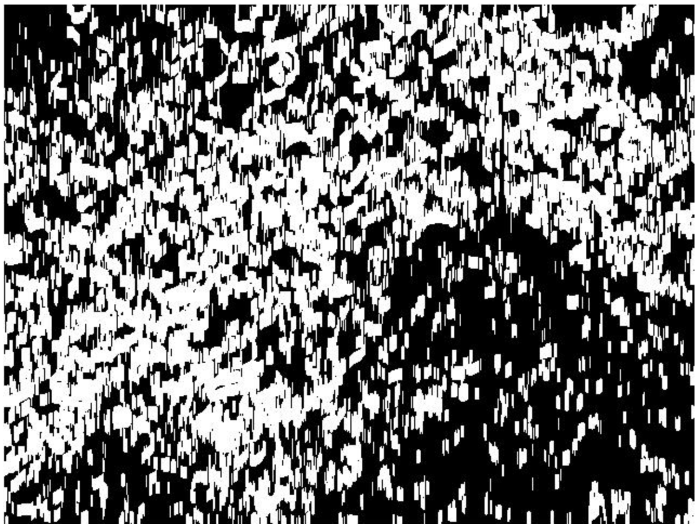
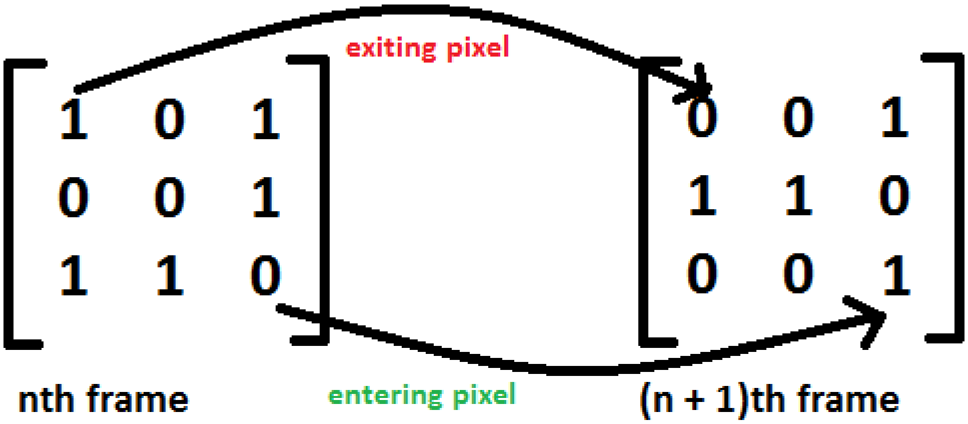


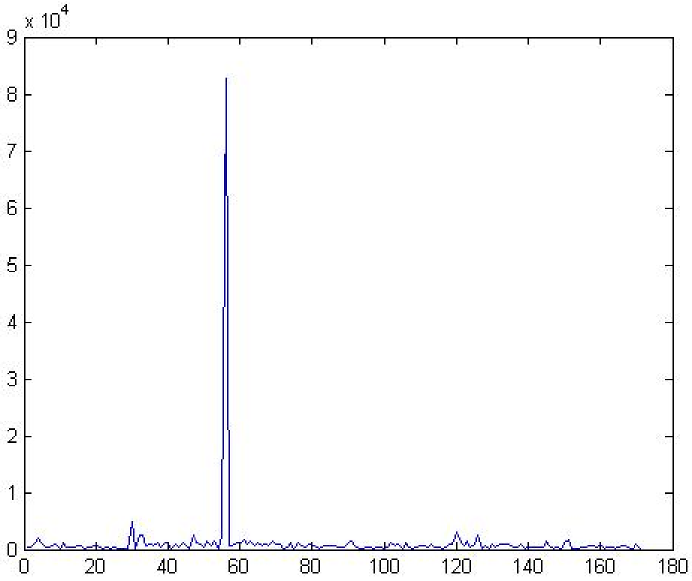
Image after dilation

- Then we check the change in edges between nth and (n + 1)th frame. There will be some pixels which were 1 in nth frame but are 0 in (n+1)th frame. Those pixels are called exiting pixels. Similarly, the pixels which turned to 1 from 0 are called entering pixels.



$$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

- We'll compute the edge change fraction by maximum of entering and exiting pixel values, and store this value in an array.
- Then the array will be plotted. If we get sudden peaks in the plot, it means that video has been tampered.



Peak is detected which is a sign of tampered video

4.2 Content Authentication

Watermarking is a technique used to hide data or identifying information within digital multimedia. Watermarking is becoming popular, especially for adding undetectable identifying marks, such as author or copyright information.

Watermarking techniques can be classified as:

- Text Watermarking
- Image Watermarking
- Audio Watermarking
- Video Watermarking

In other way, the digital watermarks can be divided into three different types as follows:

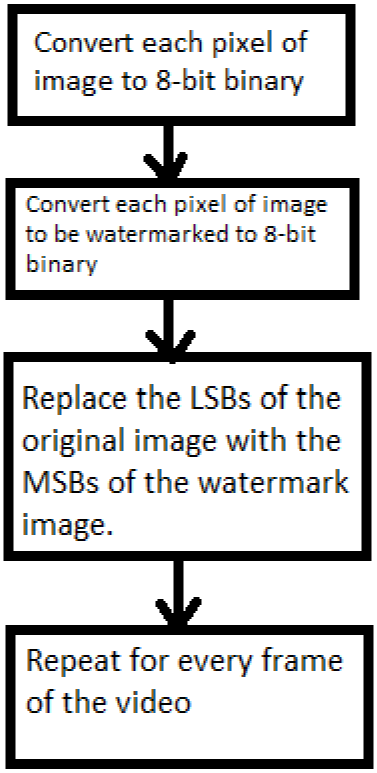
- Visible watermark
- Invisible-Robust watermark
- Invisible-Fragile watermark

4.2.1 Least Significant Bit (LSB) Watermarking

The idea behind this watermarking technique is the following: if you see you image as a matrix NxM (where N and M are the dimension of the image) you can represent the value of the pixel in the position (i,j) as a binary number. As grayscale value ranges from 0-255, every pixel is a 8 bit binary number.

The first 4-bits are called Most Significant Bits (MSB) and last 4-bits are called Least Significant Bits (LSB).

MSBs have more than 80% data of your image. We use this property of image to watermark new image in it.


Convert each pixel of image to 8-bit binary
Convert each pixel of image to be watermarked to 8-bit binary
Replace the LSBs of the original image with the MSBs of the watermark image.
Repeat for every frame of the video

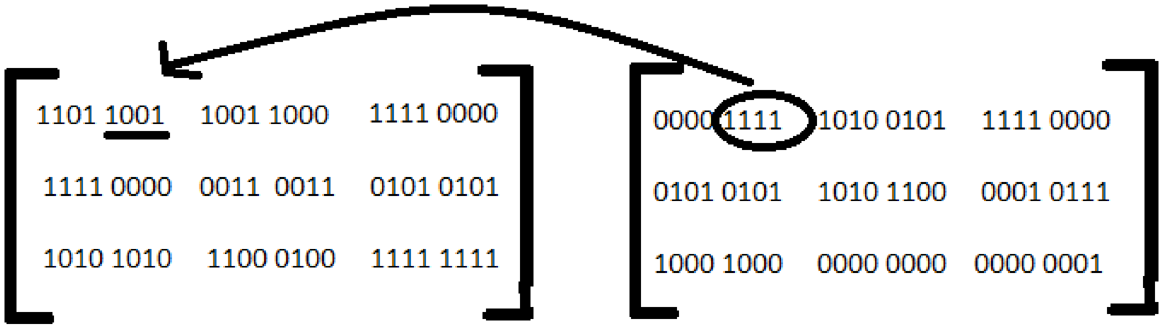
Flowchart of the algorithm

- Remove the LSBs of each pixel of image by applying right shift four times. If our pixel value is 20. Its binary representation is 0001 0100. After applying right shift 4 times, the new binary value will be 0001.
- Remove the LSBs of each pixel of watermark image by same method. You'll be left with MSBs of the watermarked image.
- Now insert these 4 bits at the right of the corresponding image pixel.

- If the 4 bits of watermark image are b1, b2, b3, b4 (left to right) and IM be the value of pixel of the original image, the new value will be

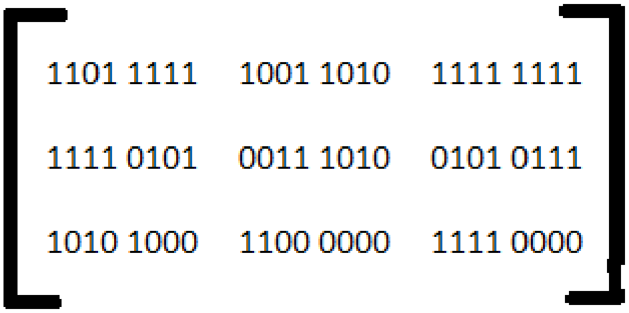
$$IM = (((((IM * 2) + b1) * 2 + b2) * 2 + b3) * 2 + b4)$$

- After all the frames are watermarked, combine them and create the video.
- Retrieval can also be done in the same way by extracting LSBs of watermarked image.



$$\begin{bmatrix} 1101\ \underline{1001} & 1001\ 1000 & 1111\ 0000 \\ 1111\ 0000 & 0011\ \ 0011 & 0101\ 0101 \\ 1010\ 1010 & 1100\ 0100 & 1111\ 1111 \end{bmatrix} \qquad \begin{bmatrix} 0000\ 1111 & 1010\ 0101 & 1111\ 0000 \\ 0101\ 0101 & 1010\ 1100 & 0001\ 0111 \\ 1000\ 1000 & 0000\ 0000 & 0000\ 0001 \end{bmatrix}$$

Original image **Watermark image**



$$\begin{bmatrix} 1101\ 1111 & 1001\ 1010 & 1111\ 1111 \\ 1111\ 0101 & 0011\ 1010 & 0101\ 0111 \\ 1010\ 1000 & 1100\ 0000 & 1111\ 0000 \end{bmatrix}$$

Final image after watermarking

5. Description of Hardware and Software Used

To be used efficiently, all computer software needs certain hardware components or other software resources to be present on a computer . These prerequisites are known as **system requirements** and are often used as a guideline as opposed to an absolute rule. Most software defines two sets of system requirements: minimum and recommended. With increasing demand for higher processing power and resources in newer versions of software, system requirements tend to increase over time. Industry analysts suggest that this trend plays a bigger part in driving upgrades to existing computer systems than technological advancements.

5.1 Hardware requirements:-.

The hardware requirements are as follows:-

1. At least 20 GB of hard disk
2. 1 GB or more RAM
3. Graphics card
4. i3 processor or later

5.2 Software requirements:-

The softwares required are as follows:

1. windows operating system(Platform)
2. windows movie maker
3. matlab (image processing toolbox)
4. video splitter

6. Activity Time Chart

Activities	Before Mid-Sem	After Mid-Sem
Literature Survey	Completed	Completed
Learning Tools	MATLAB	MATLAB
Work done	• Frame Extraction • Converting to grayscale image • Binarization • Finding edges	• Edge change fraction computed • Detecting Peaks • Authenticating video

7. Results

- Algorithm which we had used is giving accuracy of 88% correct results for tamper detection.

- Optimization is done by image dilation.

- Out of 12% failed outputs, almost 80% detected fault at wrong frame while 20 % didn’t detect fault at all.

- We are able to embed the watermark in our videos successfully which helped us to authenticate our videos thus authentication of videos is done and giving 100 % results.

8. Conclusions

Video authentication is a very challenging problem and of high importance in several applications such as in forensic investigations of digital video for law enforcement agencies, video surveillance and presenting video evidence in court of law.

However with growing development in video editing tools and wide availability of these powerful editing software, video tampering attacks explores new dimensions in various fields. It becomes difficult to deal with the authenticity of raw video sequences.

A practical system of digital video watermarking is suggested for authenticating and tampering detection of compressed videos. To design an efficient and low complexity method, the embedding and extracting of watermarks are integrated with the coding and decoding routines of the video codec.

9. References

[I] F. Hartung, B. Girod, Watermarking of uncompressed and Compressed Video, S*ignal Processing 66* (1998), pp.283-301

[2] B. Mobasseri, Direct Sequence Watermarking of Digital Video using m-frames, *Proc. IEEE ICIP98*, October 4-7, 1998 Chicago

[3].B. Mobasseri, A spatial video watermark that survives MPEG , *IEEE International Conference on Information Technology: Coding and Computing*, March 27-29,2000, Las Vegas

[4] http://www.mathworks.in/ Dated 30 November 2014

[5] http://www.web.iitd.ac.in/sumeet/Jain.pdf

[6] Digital Image Processing by E. Woods and Gonzalez